

企业服务总线监听器的研究与设计^①

白莎出拉^{1,2}, 廉东本², 李文博²

¹(中国科学院 研究生院, 北京 100049)

²(中国科学院 沈阳计算技术研究所, 沈阳 110168)

摘 要: ESB 系统是基于 SOA 架构实现应用集成的软总线。监听器是 ESB 的一个重要部件, 监听器的研究与设计对 ESB 的性能及可用性有着重要影响。其主要任务是监听服务的发布消息与服务请求/响应消息, 对消息进行访问控制即消息认证。提出了较高效率的并发监听技术和安全的消息适配技术, 解决了基于多种协议类型消息的并发监听的效率问题; 对 ESB 内部消息的安全认证技术进行了深入研究并提出了一个安全性较高的设计方案。

关键词: 企业服务总线; 监听器; 高度并发性; 安全认证; webservice

Research and Design of the Enterprise Service Bus Listener

BAI Sha-Chu-La^{1,2}, LIAN Dong-Ben², LI Wen-Bo²

¹(Graduate School, Chinese Academy of Sciences, Beijing 100049, China)

²(Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China)

Abstract: ESB system is a software bus which based on SOA architecture to achieve application integration. Listener is an important component in ESB system, whose research and design have an important impact on the performance and availability of the ESB. The main task of listener is monitoring the service-dissemination messages and service request/response messages, in addition, it provides access-controlling and Message-authentication. This paper raises an more efficient concurrent monitoring technology and a safety way of the message-adapting technology. These technologies have solved the problem of the efficiency of the concurrent monitoring of multi-protocol messages; and have made a deep study in secure authentication modules of the ESB internal message and have raised a high security design.

Key words: enterprise service bus; listener; high-degree concurrency; safety certification ; webservice

随着科学技术的发展, 针对企业日益增长的信息共享和业务的需要, 部署企业服务总线(ESB)集成企业的各类异构应用是必然发展趋势。随着 SOA 理论的发展, 各种与 SOA 有关的规范和标准的不断出现 SOA 变得很成熟。监听适配部分是 ESB 的一个核心部分, 绝大部分服务的交互都通过监听器的监听和过滤来实现, 近年来业界对 ESB 中监听适配技术进行了大量的研究, 它们的研究侧重于基于少数协议类型的连接和简单适配过程的实现, 对目前越来越多的协议类型, 监听的效率、适配能力及安全性等方面仍欠缺考虑。

1 相关原理

面向服务架构(SOA) 将应用程序即服务提供者和

服务申请者通过这些服务提供者和服务申请者之间定义良好的接口和契约联系起来。接口是采用中立的方式进行定义的, 它应该独立于实现服务的硬件平台、操作系统和编程语言。这使得构建在各种这样的系统中的服务可以以一种统一和通用的方式进行交互。

企业服务总线(ESB)作为服务消息路由中间件, 在 SOA 应用中作为一种解决 Web 服务调用之间紧耦合关系的处理方式, 目前在 SOA 应用中取得了普遍共识。初级的 ESB 仅支持简单的消息转发配置, 支持更复杂的商业路由规则的 ESB 目前还处于不断的进化中。所以设计并实现一个其并发性, 可扩展性, 安全性都较高的 ESB 系统是目前很需要的。

目前 XML 和 Web Service 标准化的开放性使企业

① 基金项目: 国家水体污染控制与治理科技重大专项(2012ZX07505003)

收稿时间: 2012-07-24; 收到修改稿时间: 2012-08-24

能够在部署的所有技术和应用采用 SOA. Web Service 使应用功能得以通过标准化接口(WSDL)提供服务,并可基于标准化传输方式(HTTP 和 JMS)通信,采用标准化协议(SOAP)进行服务申请和服务结果反馈. Web 服务规范通常归为两类:基本 Web 服务规范和扩展 Web 服务规范. 基本规范包括 SOAP, UDDI 和 WSDL 等, 扩展规范则有包括 WS-BPEL 在内的数十种 WS-*规范. 本文研究的 ESB 系统中采用了 Web Service 的 WSDL 和 WS-Addressing 规范等一些技术.

ESB 的功能可以简单概括为这几个方面: 在服务与服务之间路由消息; 在请求者与服务器之间转换传输协议; 在请求者与服务器之间转换消息格式; 处理来自于各种异构源的业务事件. ESB 的整个系统框架如图 1 所示:

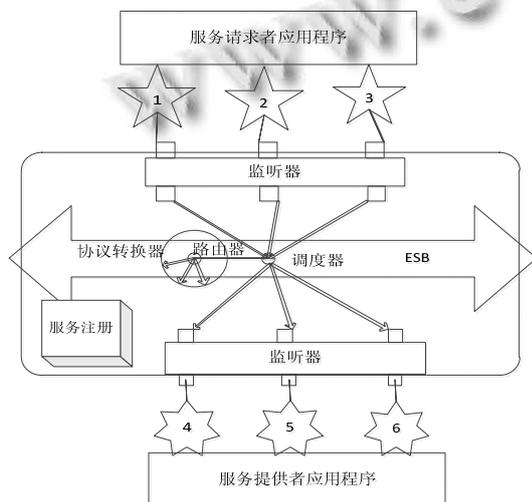


图 1 ESB 的系统框架

监听器包括监听与适配两个部分, 它的监听部分能够高效率的完成消息的监听、建立连接、传递; 它的适配部分能完成服务提供者与服务申请者的合法判断, 并对消息内容进行协议格式解析并将过滤后的消息传给调度器. 从 ESB 的角度来看, 我们在 ESB 内部使用一个标准的监听器, 一个高性能、多线程的监听器, 它能够支持来自接入方的高负荷传入消息、对请求/响应消息进行并发处理.

ESB 监听器采用消息触发机制. 根据请求消息通信协议的不同, 每个应用程序使用一种特定的端口类型来连接 ESB, 端口类型由应用程序使用的通信协议确定, 应用程序常用的通信协议有 HTTP、JMS、SMTP、IIOP、FTP 等. 传统的单线程、单端口模式只

能以串行模式工作无法满足需求. 因此 ESB 内核启动多个服务请求监听器线程, 分别对多个端口并行监听, 从而有效均衡各个端口的负载, 并在后期对消息进行协议转换时减少了统一对其进行协议类型分析的过程, 从而提高了系统的响应速度. ESB 系统除了支持各种端点协议还支持各种交互方式, 如请求/相应模式、请求/多响应模式以及事件传播模式.

2 关键技术

实现网络监听有以下几个关键步骤: 将网卡设为混杂模式; 通过 socket 端口接收数据流, 生成数据包; 数据包的分析、统计及其它处理. 监听器的基本功能实现, 主要包括三个类: 首先, 是系统主类, 它的功能是获取主机 IP; 生成监听器对象, 设置过滤条件, 过滤不符合要求的消息; 定义事件函数, 对收到的消息进行缓存, 以便进一步处理如统计、内容分析等; 并启动监听器. 其次是监听器类, 它的功能是定义 socket 对象, 实现异步网络数据流的接收; 对监听到的信息(字节流)生成“包对象”; 进行过滤判断, 对未被过滤的包, 触发相关事件. 第三个类是数据包类, 它的功能是根据网络封包的格式, 解析收到的字节流, 解析出包头各部分和包体信息.

为了实现服务总线监听器的高并发性, 安全稳定性, 以及高效率解析并传递消息, 能够支持丰富的传输协议, 本文提出了几种解决方法.

2.1 监听功能模块的设计

监听器采用线程池技术, 而且 ESB 通过不同的端口监听基于不同通信协议类型的消息. 线程池统一了处理系统性能和大量用户请求之间的矛盾, 通过对多个任务重用已经存在的线程, 降低了对线程创建和销毁的开销, 当用户请求到达的时候, 线程对象已经存在, 服务器就能立即处理客户请求, 从而提高了服务器的响应能力. 监听器提供配置管理功能, 用来配置参数信息: 各个组件的功能接口都是可配置的. 比如, 可对 Socket 的 IP 地址及端口, 线程池的大小, 连接配置等, 此功能采用管理配置文件方式实现^[1]. 具体思想如下:

服务请求者生成服务请求后, 根据自己使用的发送消息的协议类型选择对应的端口发送请求.

所有监听器线程都处于活动状态, 一旦从对应端口接收到服务请求, 立即处理. 本文只介绍监听五种

协议类型的监听方法, 有 5 个监听器线程, 端口号从系统未使用的端口随意定义, 若一个服务请求的处理时间为 t (均值), 则系统最多可以同时处理 5 个服务请求, 系统处理服务请求的平均时间为 $t/5$, 平均时间随线程数的增大而减小. 因此, 系统具有较好的并行性, 能够满足一定的及时性需求^[2].

企业服务总线系统启动时监听器主线程负责线程池的初始化, 包括线程的创建, 还负责监听各端口并且单独调用 `accept` 负责接收客户端的连接请求, 并将每个客户连接加入连接队列; 任务分配器负责从连接队列里取出连接请求, 并且从空闲线程队列中唤醒一个线程处理这个连接请求; 被唤醒的空闲线程成为了工作线程, 工作线程是循环执行任务的线程, 在没有任务的时候成为空闲线程, 并且阻塞等待^[3].

来自每一个端口的消息对应一个消息队列和一个调度管理器线程池. 各种协议优先级的高低是通过调度管理器线程池中的线程数量的多少来反映的. ESB 系统通过预先统计再设置每个线程池的大小, 如果默认情况下哪种协议类型的请求消息多, 对应的线程池线程数量就越多, 消息队列中的消息处理速度也就越快. 任务分配器从连接队列取消息的优先级也是根据此优先级进行的.

Webservice 的 WS-Addressing 规范为以同步或异步方式传输的消息提供了一种统一的寻址方法. 异步消息处理操作会极大的提高服务总线的处理性能. 服务请求消息通过监听适配时根据 WS-Addressing 规定消息编号, 对请求消息进行注册, 消息经过协议转换和路由之后根据 WS-Addressing 规范的 `<wsa:to>` 元素的属性得到它需要的服务并解析 WSDL 文件后将消息

发给对应的服务提供者之后回收分配的线程, 将此线程放入线程池中供其他任务分配, 等待响应消息的到来. 监听到响应消息后从工作线程池中配线程, 解析响应消息, 根据 WS-Addressing 规范中的 `<wsa:ReplyTo>` 元素查找到该响应消息对应的请求消息注册项, 并对响应消息进行处理. 将响应消息发给请求者. 回收分配的线程, 将此线程放入线程池中供其他任务分配. 监听器的基本结构如图 2 所示.

2.2 适配功能模块的设计

2.2.1 消息头解析

适配器提供基于消息格式的合法认证功能, 消息请求已经建立了连接之后要对消息进行消息格式的合法验证. ESB 系统对消息进行协议解析, 此时需要系统提供的标准协议库, 通过调用协议库判断消息的格式是否合法. 协议解析的过程就是对每个数据包进行逐层解码, 在每层解码后进行相关字段的过滤. 每层协议头中必定定义了某个字段如 `eth.type`、`ip.proto`、`ppp.code` 等指示如何解析该层携带的上层数据包. 具体解码做法就是参考协议的 RFC 文档, 使用 `unpack` 逐层解码、计算生成每层关键字段. ESB 监听器内部的协议解析具体步骤如下:

系统将为每个给定协议提供一个协议处理器组件. 因此, 我们将为 HTTP、SMTP、IIOP 等协议提供独立的协议处理器. 这些协议处理器的用途是提取消息头. 然后, 将提取的消息头发送到另一个称为格式检测器(FD)的软件组件. 此软件组件负责确定并检查这个消息头是否是本协议处理器指定的协议, 并过滤掉包含不合法消息头的消息. 返回一个提示“未知的消息类型”的错误消息.

2.2.2 用户认证

适配器提供基于角色的安全认证功能, 当消息已经通过消息格式的合法认证后要对角色的访问权限进行验证, 将没有访问权限的消息按错误消息处理.

消息通过添加来自外部数据源的信息(如由 ESB 定义的自定义参数或者来自数据库查询的自定义参数)来增加消息的有效负载. 当服务请求者试图访问某个服务的某个资源时, 请求消息首先得经过 ESB 系统中的统一认证服务 (UniformAuthenticationService, UAS) 模块, UAS 根据服务请求消息携带的用户凭证在用户注册表中进行搜索, 如果身份和访问权限认证成功, UAS 创建安全断言标记语言(Security Assertion

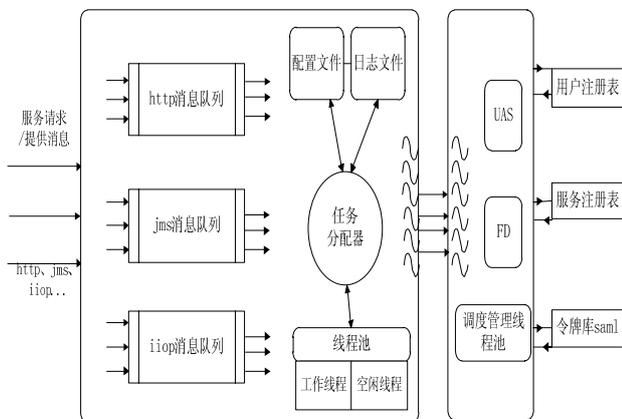


图 2 ESB 监听器结构图

Markup Language, SAML)令牌, 并返回 SAML 令牌给服务请求消息, 服务请求消息就可以携带这个 SAML 令牌访问服务^[4]. 如果用户未注册或权限不够则返回一个提示“没有访问权限或用户未注册”的错误消息.

图 3 以 http 请求消息为例来描述消息的适配过程. 如图中所示, http 消息包含请求行、消息头、消息体. 请求消息与响应消息具体包含内容也有区别. 比如响应消息头包含状态码, 而请求消息则没有. 消息经过 UAS 后其消息头中就会携带安全令牌. 在经过消息处理器就被取出消息头对其进行格式检测^[5].

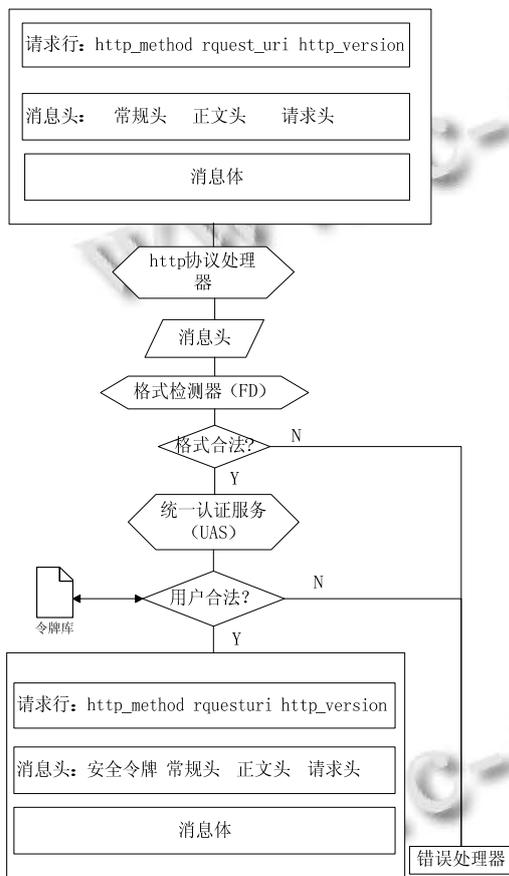


图 3 http 请求消息适配流程图

企业服务总线控制器采用基于角色的访问控制进行对消息的格式进行认证和对用户身份和权限进行认证和授权, 同时采用加密解密和来实现企业服务总线的传输安全. 保证被交换的信息不被窃听, 只有能够提供适当身份证明的人才能访问服务, 保证消息在传输中不会被有意或无意的修改.

3 结语

本文主要介绍了一种实现企业服务总线系统的提供服务过程中消息的并发监听方案以及提出了消息的访问控制. 通过基于线程池的多端口监听技术及基于令牌的用户访问授权技术可以很好的解决 ESB 系统的并发消息处理及安全性问题, 并且若结合集群技术可实现海量的消息并发处理. 目前该解决方案已应用到国家水体污染控制及治理重大专项中, 并很好的实现了 ESB 系统监听的需求. 随着 SOA 技术的成熟, ESB 系统必然越来越广泛的应用到各企事业单位中, 也必将涌现出更多的有关提高 ESB 系统中监听性能的方案.

参考文献

- 1 宋敬彬, 孙海滨. Linux 网络编程. 北京: 清华大学出版社, 2010.436-440.
- 2 曹中洪, 廉东本. 面向 SOA 的企业服务总线研究与应用. 计算机系统应用, 2010, 19(10): 63-67.
- 3 闫鹤. 海量存储系统 Web 代理服务器的设计与实现[硕士学位论文]. 上海: 上海交通大学, 2011.28-32.
- 4 李福林, 徐开勇, 李立新. 基于 ESB 的统一身份认证系统设计与实现. 计算机应用, 2012, 32(1): 52-55.
- 5 罗志伟, 汪厚祥, 井小沛. 基于 ESB 的安全管理模型研究. 计算机与数字工程, 2011, 6: 90-92.
- 6 Bean J. SOA and Web Services Interface Design. Principles Techniques and Standards. 2010.